REMARKS

In the outstanding Office Action, the Examiner rejected claim 10 under 35 U.S.C. § 112, second paragraph; and claims 10-12 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,999,629 to Heer et al. ("Heer") in view of U.S. Patent No. 6,421,779 to Kuroda et al. ("Kuroda").

By this amendment, Applicants have amended claims 10-12. Claims 10-12 remain pending in this application.

I. Rejections under 35 U.S.C. § 112, second paragraph

Regarding the rejections of claim 10 under 35 U.S.C. § 112, the Examiner first asserts that "[i]t is unclear what specific key is shared with the another device, the first key or the second key and whether another device encompasses 'a decoding means.'" Office Action, pages 2-3. Although Applicants do not agree with the Examiner's assertion, Applicants have amended claim 10 in an attempt to expedite prosecution. Specifically, claim 10 has been amended to recite an information processing device including "decoding information received from a remote device, the information being encoded with a first key and the first key being encrypted by a second key." That is "information" is "received from a remote device," wherein that "information" is "encoded with a first key," and the "first key" is "encrypted by a second key." Accordingly, the "first key" is transferred from a remote device, and received by the "information processing device." Moreover, "another device" cannot constitute "a decoding [unit]," because "the information processing device . . . comprises a security unit and a decoding unit." That is, Applicants claimed "security unit" and "decoding unit" are contained in the same "information processing device."

The Examiner further rejects claim 10[1] under 35 U.S.C. § 112, second paragraph for omitting essential structural cooperative relationships of elements, stating, "[i]t is unclear whether Applicant claims a software module that store sin the memory (storage means)." Office Action page 3. Applicants respectfully disagree with the Examiner's assertion. In an attempt to expedite prosecution, however, Applicants have amended claim 10 to remove recitations of "a storage means." Accordingly, claim 10 recites "[a]n information processing device . . . comprising: a security unit and a decoding unit." That is, claim 10 is directed towards an "information processing device" that comprises both "a security unit" and "a decoding unit," wherein essential structural cooperative relationships are described therebetween.

For at least the foregoing, Applicants submit that claim 10, as amended, complies with the second paragraph of 35 U.S.C. § 112. Accordingly, Applicants respectfully request that the Examiner withdraw the rejection of claim 10 under 35 U.S.C. § 112, second paragraph.

II. Rejection under 35 U.S.C. § 103(a)

Applicants respectfully traverse the Examiner's rejection of claims 10-12 under 35 U.S.C. § 103(a) on the ground that a *prima facie* case of obviousness has not been established. A *prima facie* case of obviousness has not been established for at least the reason that Heer and Kuroda, taken alone or in combination, fail to teach or suggest every feature recited in claims 10-12. For example, Heer fails to disclose an information processing device including "first encrypting/decrypting means for . . . encrypting the

[1] On page 3 of the Office Action, the Examiner rejects claim 1 under 35 U.S.C. § 112, as allegedly being incomplete for omitting essential structural cooperative relationships of elements. Because claim 1 has been canceled, Applicants have assumed that the Examiner meant to reject claim 10.

first key with the temporary key," and "transmitting means for transmitting the encrypted first key and the temporary key . . . to the decoding unit," as recited in claim 10.

Heer discloses "security module 30 . . . encrypts each of the program encryption keys using S_{local}" (col. 3, lines 36-38), and "when IPS 20 receives an instruction via path 21 from ACS 40 or user terminal 27 to encrypt a video program that will be received via path 16, then processor 25 unloads one of the encrypted program encryption keys . . . and supplies the encrypted program encryption key and identifier to security module 30" (col. 3, lines 45-50). This encrypted program encryption key is then used to encrypt the video program. *See*, Heer, col. 3, lines 51-61. Moreover, "[s]ecurity module 30 . . . uses S_{local} to decrypt the encrypted program encryption key that it received from processor . . . [then] encrypts the digital video stream that it receives via path using the decrypted program encryption key." Heer, col. 4, lines 5-11.

To the extent that the video program or digital video signals, the encrypted program encryption key, and S_{local} can reasonably correspond to Applicants' claimed "information," "encrypted first key," and "second key," respectively, Heer fails to disclose at least "encrypting the first key with the temporary key," and "transmitting the encrypted first key and the temporary key . . . to the decoding unit," wherein "the decoding unit decodes the information with the first key," as recited in claim 10 (emphasis added). Heer merely discloses that the digital video signals are encrypted with a program encryption key that was decrypted using the S_{local} key. Heer does not disclose that the decrypted program encryption key is re-encrypted using a temporary key.

Heer also fails to disclose "[a]n information processing device for decoding information received from a remote device, the information being encoded with a first

key and the first key being encrypted by a second key," as recited in claim 10. Heer discloses a video information delivery system 100 (*see* Fig. 1) which delivers encrypted video programs to subscriber terminals 200-1. To the extent that video information delivery system 100 of Heer can reasonably correspond to Applicants' claimed "remote device," Heer does not teach that subscriber terminal 200-1 decodes the encrypted video program in the manner described in claim 10, not does Heer disclose that the encrypted video program is "encoded with a first key and the first key being encrypted by a second key," as recited in claim 10.

Kuroda, cited by the Examiner at page 5 of the Office Action for allegedly teaching "the second authentication means for authenticating the first storage means," fails to cure the above-noted deficiencies of Heer. In Kuroda, a "DES process is performed on the first 64-bit block M2 in step S51 [and] the DES process is performed again on the result using a master key." Kuroda, col. 13, lines 41-46. Kuroda then teaches, "a receiver of a storage certificate can decode the data using the master key." Kuroda, however, is silent as to a "temporary key," and thus fails to provide a teaching of ""encrypting the first key with the temporary key," and "transmitting the encrypted first key and the temporary key . . . to the decoding unit," as recited in claim 10.

Because nether Heer nor Kuroda teach or suggest every element recited in claim 10, even if combined as suggested in the Office Action, that combination of references cannot establish a *prima facie* case of obviousness. Accordingly, Applicants respectfully request that the Examiner withdraw the rejection of claim 10 under 35 U.S.C. § 103(a).

Claims 11-12, although of different scope, recite features similar to those discussed above for claim 10. Claims 11-12 are thus allowable over Heer and Kuroda for at least the reasons given above with respect to claim 10. Accordingly, Applicants respectfully request that the Examiner withdraw the rejection of claims 11-12 under 35 U.S.C. § 103(a).

In view of the foregoing amendments and remarks, Applicant respectfully requests reconsideration and reexamination of this application and the timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: November 15, 2006

By: _____
Darrell D. Kinder, Jr.
Reg. No. 57,460